Claims

What is claimed is:

1. A method for performing mutual authentication and authorization of a user's terminal device (U) and an Internet Service Provider (P) in order to establish secure communication between the terminal (U) and a trusted gateway (T) to the Internet via an untrusted access station (A) comprising:

establishing an association between a terminal (U) and an untrusted access station (A);

transmitting an ISP authentication packet from terminal (U) to ISP (P) via the untrusted access station (A);

sending a user authentication packet from said ISP (P) to said terminal (U) via said untrusted access station (A);

upon authentication of said terminal (U) and said ISP (P), said ISP performs the following:

generating a session key;

distributing said session key to said terminal (U) and a trusted gateway (T), wherein said session key is used to encrypt traffic between the terminal (U) and the trusted gateway (T);

establishing a secure tunnel such that the terminal (U) may communicate with the Internet via said trusted gateway (T);

wherein said secure tunnel emulates a physical link between the terminal (U) and the trusted gateway (T) such that traffic transmitted between the terminal (U) and said Internet via said trusted gateway (T) is secure from modification or eavesdropping by said third party access station (A).

2. The method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted gateway to the Internet (T) via an untrusted access station (A) of claim 1, wherein the ISP (P) authentication packet contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P).

3. The method for performing mutual authentication and authorization of a terminal (U) and an Internet Service Provider (P) in order to establish a secure tunnel between the terminal (U) and a trusted gateway to the Internet (T) via an untrusted access station (A) of claim 1, wherein the user authentication packet contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of user (U).

4. A method for providing public access to IP-based networks via an untrusted infrastructure having untrusted access points comprising:

establishing a connection between an IP-device (U) and said untrusted access point (A), wherein an IP address is dynamically allocated to said IP device;

transmitting an ISP authentication request from said IP device (U) to an internet service provider (P) affiliated with said IP device (U), wherein said authentication request

is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure;

transmitting a user authentication request from said ISP (P) to said IP device (U) to determine whether said IP device (U) is a valid user affiliated with said ISP (P), wherein said authentication request is transmitted through said untrusted access point (A) affiliated with said untrusted third party owned infrastructure;

when said ISP (P) authentication request and said user authentication requests is affirmative, said ISP (P):

generates a key session for encrypting data packets; and

distributes said session key to said IP device (U) and a trusted node (T), wherein said session key is used to encrypt data transmitted between said IP device (U) and said trusted node (T);

establishing a secure tunnel as said session key is used to encrypt data packets transmitted between said IP device (U) and said trusted node (T), such that said data packets transmitted between said IP device (U) and an Internet via the untrusted access station (A) are protected from modification and manipulation by said untrusted access station (A) in said secure tunnel.

5. A method for providing public access to IP-based networks through a third party owned, untrusted infrastructure having untrusted access stations (A) comprising:

establishing a connection between an IP-device (U) and said access station (A), wherein an IP address is dynamically allocated to said IP device (U);

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P);

sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P);

upon affirmative authentication of said ISP (P) and said IP device (U);

establishing a trusted connection between said IP device (U) and a trusted gateway (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services.

6. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over a third party owned untrusted access station (A) comprising:

establishing a connection between the terminal (U) and said access station (A);

sending an ISP authentication request to said internet service provider (P) affiliated with said terminal (U);

sending a user authentication request from said ISP (P) to said terminal (U);

upon affirmative authentication of said ISP (P) and said terminal (U):

establishing a trusted connection between said IP device (U) and a trusted gateway (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of resource in said untrusted access station (A) in order to provide the IP device (U) with prescribed for services.

7. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP authentication request contains an authentication challenge (CH_U) from terminal (U) to ISP (P) to authenticate the identity of ISP (P).

8. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the user authentication request contains an authentication challenge (CH_P) from ISP (P) to the terminal (U) to authenticate the identity of terminal (U) as having subscribed to said ISP (P) for services.

9. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, the ISP (P) generates a session key for encrypting data packets upon the affirmative authentication of the terminal (U) and the ISP (P).

10. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) selects a trusted node (T) with said Internet.

11. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the

Internet over an untrusted access station (A) of claim 9, wherein said ISP (P) distributes said session key to the terminal (U) and the trusted node (T).

12. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the session key is used to encrypt data packets transmitted between the terminal (U) and the trusted node (T).

13. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 12, wherein the transmission of encrypted data packets between the terminal (U) and the trusted node (T) established a secure tunnel.

14. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 13, wherein the secure tunnel protects the data packets from manipulation by said untrusted access station (A).

15. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, a time out is distributed to the trusted node (T) and terminal (U) upon the establishment of a secure tunnel.

16. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the

Internet over an untrusted access station (A) of claim 15, wherein the timeout value is set to a predetermined time period, wherein if the secure tunnel is active for a time period equal to the timeout value, the secure tunnel will expire and the resources utilized for the secure tunnel will be releases.

17. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T) decrypts the data packet and forwards the decrypted data packet to the Internet.

18. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 17, wherein upon receipt of an encrypted data packet from the terminal (U), the trusted node (T) decrypts the data packet and forwards the decrypted data packet to a remote communication peer (R).

19. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein the Internet sends an original data packet to the terminal (U) via the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A).

20. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the

Internet over an untrusted access station (A) of claim 17, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the Internet.

21. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 18, wherein a remote communication peer (R) sends an original data packet to the terminal (U) via the trusted node (T), wherein the trusted node (T) encrypts the original data packet and forwards the encrypted data packet to the terminal (U) via the untrusted access station (A).

22. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 21, wherein upon receipt of the encrypted data packet from the trusted node (T), the terminal (U) utilizes the session key to decrypt the data packet thus yielding the original data packet from the remote communication peer (R).

23. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) provides an accounting of time to the untrusted access station (A) for resources utilized by the terminal (U).

24. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the

Internet over an untrusted access station (A) of claim 6, wherein the untrusted access station (A) is incorporated into a third party owned network infrastructure.

25. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the ISP (P) provides the terminal (U) with at least one subscribed for service via an untrusted access station (A).

26. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the ISP (P) reimburses the untrusted access station (A) for resources expended on the terminal (U) according to an accounting of time.

27. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 25, wherein the ISP (P) bills the terminal (U) for services provided to the terminal (U).

28. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located in the network infrastructure of a public facility.

29. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the

Internet over an untrusted access station (A) of claim 28, wherein the public facility is at least one of an airport, a convention center, a restaurant, a hotel, a library, and a school.

30. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 24, wherein the untrusted access station (A) is located within the infrastructure of a private household or within the private infrastructure of a corporation or government institution.

31. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access stations (A) is compatible with at least one wireless transmission standard including WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), or HiperLan.

32. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 32, wherein the terminal (U) is a mobile device.

33. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the terminal (U) recognizes a compatible access point by broadcasting a dynamic host configuration protocol (DHCP) request and receiving a "magic" DHCP response from the untrusted access station (A).

34. A method of establishing secure communication between a terminal (U), the Internet Service Provider (P) affiliated with that terminal and the Internet over an untrusted access station (A) of claim 6, wherein the untrusted access station (A) assigns an local unique identification (LUID) to the terminal (U) in order to facilitate matching the terminal with data packets when the untrusted access station (A) is simultaneously serving multiple terminals (U).

35. A computer program product for accessing and authenticating Internet service via an untrusted access point comprising:

software instructions for enabling the computer to perform predetermined operations, and

a computer readable medium bearing the software instructions;
the predetermined operations including

establishing a connection between an IP-device (U) and said access station (A), wherein an IP address is dynamically allocated to said IP device (U);

sending an ISP authentication request to said internet service provider (P) affiliated with said IP device (U) requesting to validate the authenticity of the ISP (P);

sending a user authentication request from said ISP (P) to said IP device (U) to validate whether said IP device (U) has a service agreement with said ISP (P);

upon affirmative authentication of said ISP (P) and said IP device (U).

establishing a trusted connection between said IP device (U) and a trusted gateway (T), wherein a secure tunnel allows the ISP (P) to dynamically obtain control of

resource in said untrusted third party owned access station (A) in order to provide the IP device (U) with prescribed for services.